

REMARKS

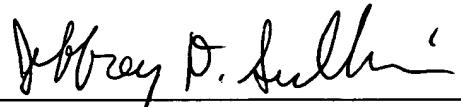
Prior to examination of the above-identified application, Applicants respectfully request to amend paragraphs [005] on page 2, [008] on page 3, and [009] on pages 3-4. In each case the text has been amended to update the names of Internet addresses where the cited references are available. It is respectfully submitted that Applicant became aware of the changes to the names of the amended Internet addresses only after submission of the application, and that the reference available under the updated Internet address name is the same as under the old Internet address name. Accordingly, it is respectfully submitted that the foregoing amendment does not constitute new matter.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "Version with markings to show changes made."

In view of the foregoing, allowance of all claims in this application is respectfully requested.

Dated: February 14, 2002

Respectfully submitted,



Jeffrey D. Sullivan  
Patent Office Reg. No. 43,170

Agent for Applicants  
(212) 408-2589

**VERSION WITH MARKINGS TO SHOW CHANGES MADE**

**In the Specification:**

Paragraph [005] on page 2 has been amended as follows:

In the context of a network including a server computer and one or more client computers having access to data from said server (as, for instance, in a World Wide Web-based webserver context), a connection depletion attack, as defined in Juels, A. and Brainard, J., *Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks*, [http:// www.rsasecurity.com/rsalabs/staff/bios/ajuels](http://www.rsasecurity.com/rsalabs/staff/bios/ajuels), 1999, first presented at the Network and Distributed System Security Symposium, San Diego, California, February 3, 1999 (hereinafter "Juels and Brainard") (herein incorporated by reference) is one in which the attacker seeks to initiate and leave unresolved a large number of connection (or service) requests to a server, exhausting its resources and rendering it incapable of servicing legitimate requests.

Paragraph [008] on page 3 has been amended as follows

Another approach, published at [http://www.rsasecurity.com/products/securid/\[datasheets/dsauthenticators\].html](http://www.rsasecurity.com/products/securid/[datasheets/dsauthenticators].html) (hereinafter "Dsauthenticators"), uses SecurID authenticators. These are hardware or software tokens each providing a sequence of one-time passwords based on a token-unique key applied successively in the

context of a proprietary algorithm. The client-side host transmits the current one-time password and a constant PIN or passphrase to a server to which it wants to identify itself. A server that possesses knowledge of the token-unique keys can synchronize with the client tokens, and thereby recognize the (remote) presence of the particular client upon receipt of the one-time password and PIN. This is a self-synchronizing system, in which the client token does not adjust its behavior based on inputs from the server on a per-transaction basis. Furthermore, the system is designed to provide entity authentication, but not authentication of the origin or integrity or the "freshness" of any ensuing communications.

Paragraph [009] on pages 3-4 has been amended as follows:

The method described in Rivest, R., Shamir, A., and Adleman, L., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the A.C.M.* 1978, 21, 120-26 (hereinafter "Rivest, Shamir and Adleman") (and enhanced based on Bellare, M., and Rogaway, P., *Optimal Asymmetric Encryption – How to Encrypt with RSA*, November 19, 1995 (revised version of Optimal Asymmetric Encryption Padding paper: <http://www-cse.ucsd.edu/users/mihir/papers/oaep.html>; earlier version published in *Advances in Cryptology – Eurocrypt 94, Lectures in Computer Science*, A. DeSantis Ed., Springer Verlag, 1994, 950, 92-111 (hereinafter "Bellare and

Rogaway") as explained further in Johnson, D. B., and Matyas, S. M., *Asymmetric Encryption: Evolution and Enhancements*, *Cryptobytes*, Spring 1996, Volume 2, No. 1 (see also [http://www.rsasecurity.com/rsalabs\[.com\]/cryptobytes](http://www.rsasecurity.com/rsalabs[.com]/cryptobytes)) (hereinafter "Johnson and Matyas") provides a means for two parties to secure the confidentiality of their communications, where the transmitting party employs the public key of the receiving party for the purpose of encryption and the receiving party employs its corresponding private key for the purpose of decryption (recovery of plaintext). The method is asymmetric in that the two parties use keys that are distinct from each other, although they are algorithmically related or paired. The method in Rivest, Shamir and Adleman can also be used to instantiate a digital signature capability, where the signing party applies its private key to the message to be signed in accordance with the method, and the verifying party applies the corresponding public key in accordance with the method in order to verify the authenticity of the origin and the integrity of the message. Digital signatures, in and of themselves, do not provide evidence of freshness; i.e., a previously used message may be replayed without being detected as a "stale" message.